37. HASIL CEK_60960140

by 60960140 Te

Submission date: 08-Aug-2022 11:51AM (UTC+0700)

Submission ID: 1880115083

File name: 37. TE-60960140-Forensik Jaringan Terhadap Serangan ARP Spoofing menggunakan Metode Live Forensic.pdf (710.84K)

Word count: 2892

Character count: 18301

InComTech: Jurnal Telekomunikasi dan Komputer
vol.10, no.2, Agustus 2020, 111-120
http://publikasi.mercubuana.ac.id/index.php/Incomtech
P-ISSN: 2085-4811 E-ISSN: 2579-6089

Forensik Jaringan Terhadap Serangan ARP *Spoofing* menggunakan Metode *Live Forensic*

M. Nasir Hafizh[1*], Imam Riadi[2], Abdul Fadlil[3]

[1]*Program Studi Magister Teknik Informatika, Universitas Ahmad Dahlan*
[2]*Program Studi Sistem Informasi, Universitas Ahmad Dahlan*
[3]*Program Studi Teknik Elektro, Universitas Ahmad Dahlan*
Jl. Prof DrSoepomo SH, Umbulharjo, Yogyakarta, 55164
*Email Penulis Koresponden : m1907048019@webmail.uad.ac.id

Abstrak:
Pada jaringan komputer, protokol yang bertugas untuk untuk menerjemahkan IP address menjadi MAC *Address* adalah *Address Resolution Protocol* (ARP). Sifat *stateless* pada protokol ARP, menyebabkan protokol ARP memiliki celah dari segi keamanan. Celah ini dapat menimbulkan serangan terhadap ARP Protocol, disebabkan karena ARP request yang dikirimkan secara broadcast, sehingga semua host yang berada pada satu broadcast domain dapat merespon pesan ARP tersebut walaupun pesan tersebut bukan ditujukan untuknya. Serangan inilah yang biasa disebut dengan ARP *Spoofing*. Serangan ini dapat berimbas pada serangan-serangan yang lain, seperti serangan *Man In The Middle Attack*, *Packet Sniffing*, dan *Distributed Denial of Service*. Metode *Live Forensic* digunakan untuk mengidentifikasi dan mendeteksi serangan ketika sistem dalam keadaan menyala. Berdasarkan hasil penelitian yang dilakukan terbukti bahwa dengan penggunaan metode *Live Forensics,* investigator dapat dengan cepat mendeteksi suatu serangan dan mengidentifikasi penyerangnya.

Katakunci:
ARP *Spoofing;*
Distributed Denial of Service;
Forensik Jaringan;
Live Forensic;
Man In The Middle Attack;
Sniffing;

Riwayat Artikel:
Diserahkan 11 Juli 2020
Direvisi 4 Agustus 2020
Diterima 9 Agustus 2020
Dipublikasi 25 Agustus 2020

DOI:
10.22441/incomtech.v10i2.8757

1. PENDAHULUAN

Semakin berkembangnya dunia teknologi informasi saat ini memudahkan pengguna dalam memberikan dan memperoleh informasi. Dunia teknologi informasi tidak terlepas dari kemajuan dunia jaringan komputer, yang memberikan banyak kemudahan dalam mengakses dan mendapatkan informasi. Pengguna dibuat terhipnotis dengan banyak fasilitas yang diberikan, sehingga tidak menyadari bahwa banyak kejahatan yang dapat terjadi dalam dunia jaringan komputer.

Cyber crime merupakan aktivitas teknologi yang melakukan kejahatan, seperti menghapus informasi, meretas jaringan, mengambil data pengguna jaringan, dan menyembunyikan informasi, dalam suatu jaringan komputer. Beberapa kejahatan

pada suatu jaringan komputer, seperti *Distributed Denial of Service* (DDoS), *Sniffing*, *Spoofing*, dan *Man In The Middle Attack*, sangat berbahaya apabila terjadi pada sebuah jaringan komputer. Kejahatan-kejahatan yang terjadi dapat mengakibatkan pencurian data, rusaknya alat komunikasi, dan terputusnya konektifitas pada jaringan. Hal tersebut sangat merugikan pengguna jaringan, karena pelaku bisa saja mendapatkan informasi-informasi targetnya secara ilegal. Adapun informasi-informasi penting yang biasanya didapat oleh pelaku, seperti informasi kartu kredit, *username* dan *password*, baik *email* atau layanan perbankan, dan data-data penting lainya.

Jaringan-jaringan dengan ruang lingkup kecil, seperti pada perkantoran, rumah, sekolah, dan lain-lain, biasanya menggun jaringan *Local Area Network* (LAN) untuk konektifitas antar perangkatnya. Setiap perangkat memiliki alamat yang berbeda-beda, yang terdiri dari IP *Address* dan MAC *Address*. IP *address* digunakan untuk mengidentifikasi tiap komputer di dalam suatu jaringan internet. MAC *Address* juga digunakan sebagai alamat fisik pada suatu perangkat jaringan yang tidak dapat diubah.

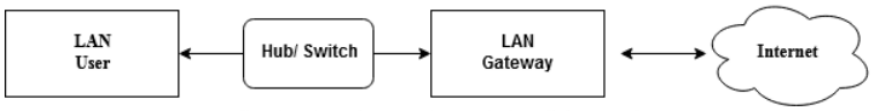
Pada penilitian terdahulu dilakukan pendeteksian serangan ARP *Spoofing* dengan memeriksa *log file* dan melakukan analisis pada paket-paket data yang beredar pada jaringan komputer [1]. Paket-paket tersebut diperiksa pada paket header, jumlah paket, sumber pengirim paket dan alamat tujuan paket. Pada penelitian lain, dilakukan penelitian pengembangan sistem keamanan jaringan komputer berdasar analisis forensik jaringan [2]. Penelitian tersebut dilakukan dengan tujuan untuk menyelidiki dan menentukan jenis serangan berdasarkan data *log*. Untuk penelitian dengan menggun metode *Live Forensic*, dilakukan penelitian terhadap serangan *Man In The Middle Attack* berbasis *Evil Twin*, dimana pada penelitian tersebut lebih fokus dari sisi penggunan [3].

Penilitian forensik jaringan telah dilakukan juga untuk mendeteksi *flooding attack* pada *web server* [4]. Pada penelitian tersebut, Peneliti menerapkan sistem pendeteksi *Intrusion Detection System* (IDS) seperti *snort*. *Snort* adalah sebuah *tools* yang digunakan untuk mendeteksi *flooding attack*. Semua aktifitas lalu lintas jaringan tersimpan didalam *log file*, kemudian dilakukan analisis atau investigasi terhadap *log file* tersebut. Pada penelitian-penelitian terdahulu terfokus terhadap serangan yang terjadi pada jaringan komputer.

Forensik jaringan adalah ilmu yang berfokus pada suatu area jaringan komputer dan perangkat-perangkat yang terhubung dalam suatu jaringan tersebut dalam upaya untuk menemukan informasi penyerang dan untuk mencari bukti atas serangan pada suartu jaringan komputer [5] [6].

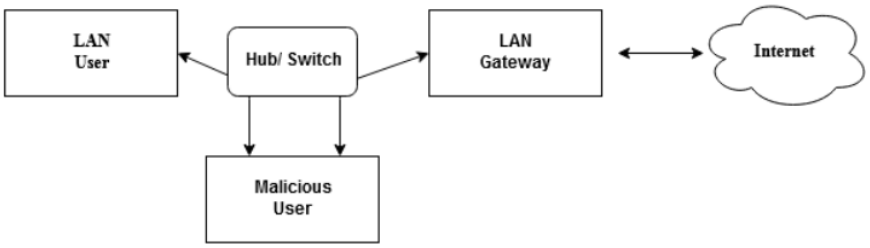
ARP *protocol* merupakan suatu *protocol* yang bekerja pada *network layer,* yang bertugas untuk menerjemahkan IP *address* menjadi MAC *Address* [7]. ARP *Spoofing* merupakan suatu kejahatan atau serangan yang dapat terjadi pada suatu jaringan dengan cara memalsukan MAC *Address* [8, 9, 10].

Jaringan LAN berjalan dengan kondisi normal ketika pengguna terhubung keperangakat *Hub*/*Swith* dan *gateway*, kemudian tersambung dengan internet dengan data tidak terlebih dahulu melalui *attacker*. Seperti yang terlihat pada Gambar 1.



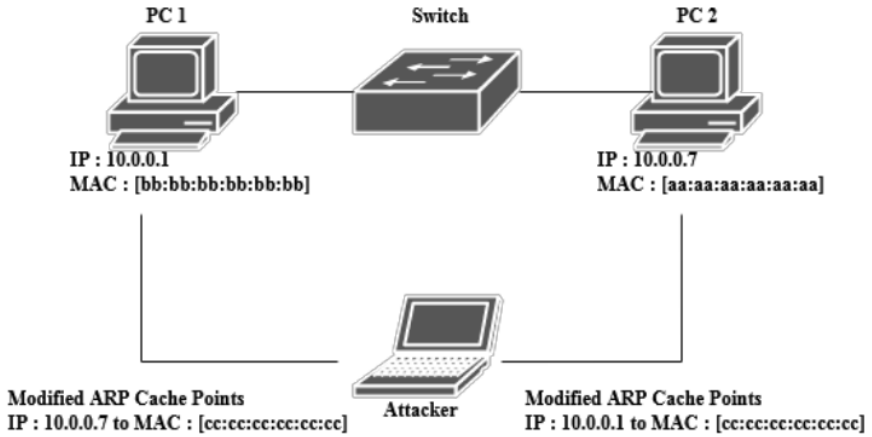
Gambar 1. Jaringan LAN pada kondisi normal

Jaringan LAN berjalan dengan kondisi tidak normal ketika terdapat *attacker*, pengguna terhubung ke internet melalui *host attacker*, sehingga paket data yang lewat dapat diambil oleh *attacker*. Kondisi ini diperlihatkan pada Gambar 2.



Gambar 2. Jaringan LAN pada kondisi terdapat *attacker*

ARP *Spoofing* pada jaringan bekerja ketika dua unit *personal computer* (PC) terhubung dalam jaringan. Masing-masing PC memiliki IP *Address* dan MAC *Address* yang berbeda. *Attacker* memodifikasi MAC *Address*, sehingga memiliki dua IP *Address* namun hanya memiliki satu MAC *Address*. Pada saat PC1 dan PC2 saling mengirim paket data, maka paket data tersebut melalui *host attacker*. Situasi tersebut diperlihatkan pada Gambar 3.



Gambar 3. Topologi Jaringan dengan ARP *Spoofing*

Log file adalah dokumentasi aktivitas yang tersimpan secara otomatis dengan *time stamps* yang relevan dengan *system* tertentu. Hampir semua aplikasi dan *system* perangkat lunak menghasilkan *file log*. *Log* dapat disebut juga sebagai *file* yang berisi daftar aktifitas yang terjadi [11].

Live Forensics merupakan sebuah metode yang digunakan untuk mengumpulkan data informasi dan barang bukti data elektronik pada suatu jaringan komputer dalam kondisi menyala. Metode ini bertujuan untuk penanganan lebih cepat [12, 13, 14].

IP *Address* merupakan deretan dari bilangan *binary* sepanjang *32-bit* yang berfungsi untuk mengidentifikasi *host* pada jaringan [15]. Pada setiap komputer yang terhubung ke internet memiliki IP *Address* yang berbeda-beda. IP *Address* disebut juga sebagai kode pengenal komputer pada jaringan atau internet. IP *Address* merupakan komponen penting dalam suatu jaringan internet, karena tanpanya suatu komputer/ *host* tidak dikenal didalam jaringan atau internet.

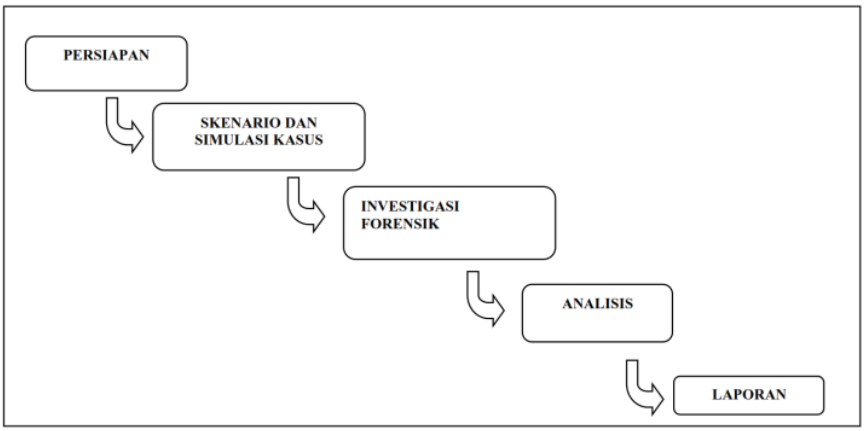
MAC *Address* adalah alamat fisik, yang mempunyai alamat yang unik, berfungsi untuk mengidentifikasi sebuah komputer, *interface*, *router* dan perangkat lainnya yang berada pada jaringan. MAC *Address* merupakan sebuah alamat yang berada pada lapisan *data-link* dalam *OSI layer* [16].

2. METODE

Pada *Forensic Digital*, terdapat beberapa tahap yang dilakukan sebelum bukti-bukti dari kejahatan *forensic* dilaporkan, antara lain seperti pengumpulan barang bukti, pemeriksaan barang bukti, dan data analisis barang bukti. Pada tahapan pengumpulan barang bukti, terdapat dua metode yang sering digunakan, yaitu metode *Dead Forensics* dan metode *Live Forensics*, masing-masing metode memiliki perbedaan dalam pengumpulan barang bukti. Metode *Dead Forensics* atau *Traditional Forensics* adalah metode yang digunakan dalam mengumpulkan barang bukti pada saat *system* dalam kondisi mati. Lain halnya dengan metode *Live Forensics*, digunakan dalam mengumpulkan data barang bukti pada saat *system* dalam kondisi menyala, dengan harapan pelaku dapat segera teridentifikasi, serta lebih cepat dalam proses penanganan.

Dalam pengumpulan barang bukti dilakukan identifikasi dan pengambilan data dari sumber data yang relevan. Pada pemeriksaan barang bukti, dilakukan pemerikasaan atau investigasi terhadap data-data yang telah didapatkan. Data-data tersebut dianalisis untuk mendapatkan informasi-informasi terkait dengan serangan yang ada pada suatu jaringan. Informasi yang didapatkan dari hasil analisis menjadi suatu laporan yang dapat digunakan sebagai acuan untuk pengambilan keputusan terkait serangan pada suatu jaringan. Keputusan dapat berupa cara mencegah dan mengatasi serangan-serangan yang ada pada suatu jaringan, sehingga pengguna jaringan merasa aman dalam melakukan aktifitas-aktifitasnya.

Adapun langkah-langkah yang dilakukan pada penelitian ditunjukkan pada Gambar 4.



Gambar 4. Tahapan Penelitian

2.1. Persiapan

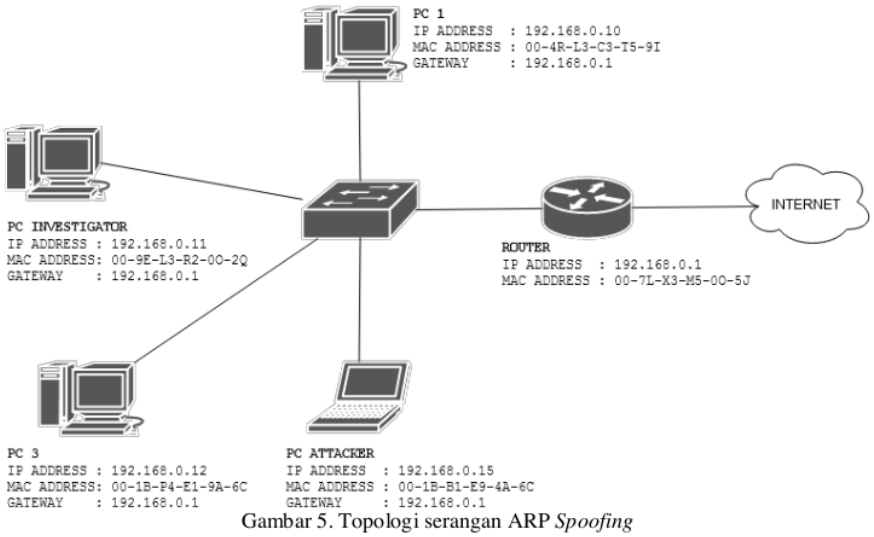
Persiapan adalah langkah pertama untuk mengidentifikasi kebutuhan-kebutuhan dalam menganalisa suatu kejadian. Dalam tahap ini terdapat dua bagian yang harus dipersiapkan. Pertama adalah persiapan *tools* yang digunakan baik *software* maupun *hardware*. Bagian kedua adalah persiapan *literature review*, yang digunakan untuk membantu Peneliti dalam hal teori-teori untuk menyelesaikan suatu kasus. Persiapan *software* dan *hardware* dapat dilihat pada Tabel 1.

Tabel 1. Tabel Persiapan Software dan Hardware

No.	*Hardware* dan *Software*	Keterangan
1	Samsung Notebook NF210 Processor Intel Atom 1.50Ghz RAM 2GB	Sebagai komputer yang digunakan untuk melakukan serangan ARP *Spoofing*
2	ASUS Notebook PC A456U Processor Intel Core i5 7th Gen RAM 4GB	Sebagai komputer yang digunakan sebagai *investigator*
3	*Wireshark*	*Network Protocol Tool Analyzer*, *tool* yang digunakan untuk menganalisa lalu lintas paket pada jaringan
4	*Ettercap*	*Tool* yang digunakan untuk *melakukan* serangan ARP *Spoofing*
5	*Cain and Abel*	*Tool* yang digunakan untuk *melakukan* serangan *Sniffing and Spoofing*
6	*X*ARP	Tool yang digunakan untuk mendeteksi adanya serangan ARP *Spoofing*

2.2. Skenario dan Simulasi Kasus

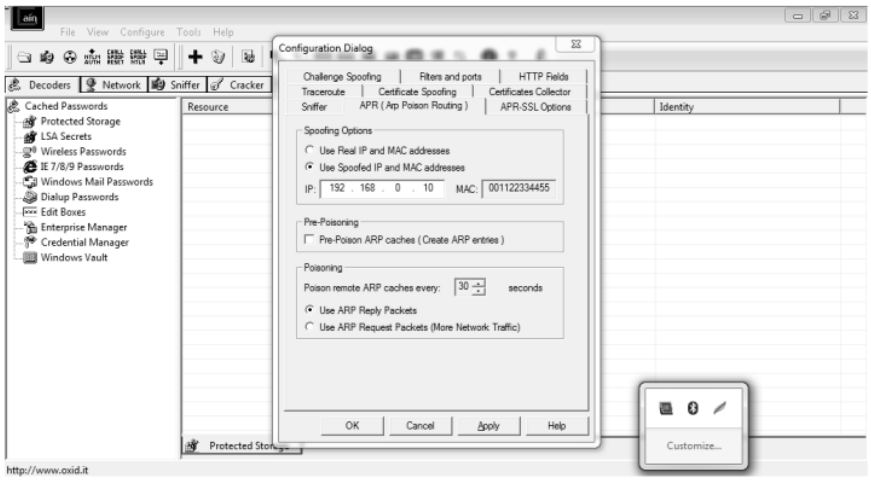
Pada tahapan ini dilakukan skenario dan simulasi serangan ARP *Spoofing* pada suatu jaringan. Jaringan yang digunakan pada tahapan ini menggun *topology star*. Topologi serangan ARP *Spoofing* terlihat pada Gambar 5.



Gambar 5. Topologi serangan ARP *Spoofing*

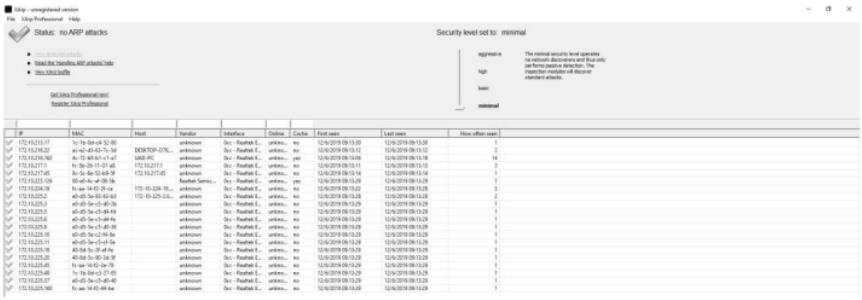
Skenario pertama, PC *Attacker* melakukan satu kali serangan ARP *Spoofing*. Skenario kedua PC *Attacker* melakukan dua kali serangan ARP *Spoofing* dalam waktu yang berbeda. Skenario ketiga, dua PC *Attacker* melakukan serangan ARP *Spoofing* dalam waktu yang sama.

Attacker melakukan serangan ARP *Spoofing* dengan menggunakan *tools* Cain and Abel yang berjalan pada Windows. Cain and Abel merupakan tools yang digunakan untuk melakukan *Sniffing* dan *Spoofing*. Dengan menggunakan *tools* ini, penyerang dapat melakukan *Sniffing* untuk mendapatkan *username* atau *password* dan juga dapat digunakan untuk melakukan *Spoofing*. Tampilan aplikasi Cain and Abel diperlihatkan pada Gambar 6.



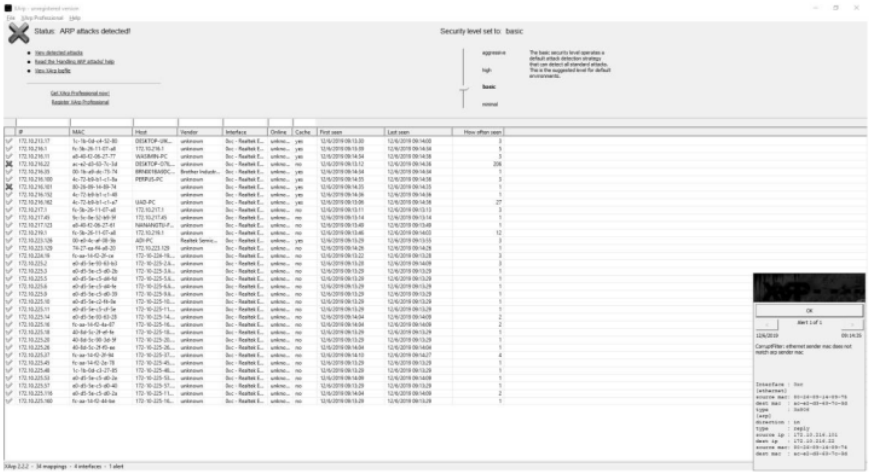
Gambar 6. Tampilan aplikasi Cain and Abel

Aplikasi XArp digunakan untuk mendeteksi dan memberikan peringatan apabila terjadi serangan ARP *Spoofing*. XArp memberikan peringatan saat serangan ARP *Spoofing* terdeteksi dan memberikan IP *Address Victim*, IP *Address Aattacker* dan waktu terjadinya serangan. Tampilan XArp pada kondisi normal dapat dilihat pada Gambar 7.



Gambar 7. Tampilan aplikasi XArp kondisi jaringan normal

XArp memberikan peringatan dini apabila terjadi serangan ARP *Spoofing* dengan memunculkan notifikasi. Proses mendeteksi serangan ARP *Spoofing* dengan menggunakan aplikasi ini cukup cepat, sehingga investigator dapat segera mengambil tindakan. Tampilan XArp pada saat mendeteksi serangan ARP *Spoofing* dapat dilihat pada Gambar 8.



Gambar 8. Tampilan aplikasi XArp saat mendeteksi serangan ARP *Spoofing*

Pada skenario simulasi ini juga ditugaskan sebuah host dengan menggun *tools* Wireshark untuk memeriksa lalu lintas jaringan, terutama pada ARP *protocol*. Wireshark digunakan untuk menganalisa lalu lintas paket data pada jaringan. Investigator dapat melihat lalu lintas data pada *protocol* tertentu. Terdapat beberapa *protocol* yang dapat dilihat pada, yaitu *protocol* ARP, TCP, dan SSDP. Tampilan pada aplikasi Wireshark dapat dilihat pada Gambar 9.

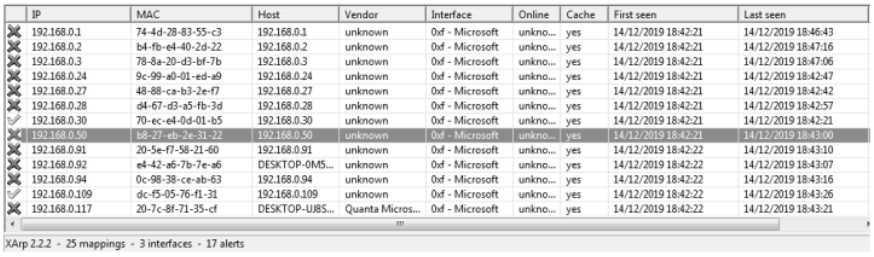
ISSN 2085-4811, eISSN: 2579-6089

Gambar 9. Tampilan aplikasi Wireshark

2.3. Investigasi Forensik

Tahapan investigasi dilakukan untuk menemukan atau mendeteksi adanya serangan ARP *Spoofing* pada suatu jaringan. Investigator menggun *tools* XArp dan melakukan *scanning* terhadap lalu lintas paket suatu jaringan untuk menemukan serangan ARP *Spoofing*. Setelah melakukan *scanning* dan menemukan adanya serangan ARP *Spoofing*, dengan menggun *tools* Wireshark, investigator melakukan proses pengumpulan data lebih detail terkait dengan identifikasi penyerang.

Pada XArp terdapat 3 *mode* yang dapat digunakan, yaitu *mode minimal*, *basic*, *high* dan *aggressive*. Pada *minimal mode*, XArp berjalan pada level minimal dengan tidak mengoperasikan penemuan serangan pada jaringan. Pada *basic mode,* XArp berjalan pada tingkat keamanan dasar dengan hanya mendeteksi serangan standar. *High mode* meningkatkan keamanan yang lebih baik dalam mendeteksi serangan jaringan, tetapi mengirimkan lebih banyak paket temuan kedalam jaringan. *Aggressive mode* memberikan tingkat keamanan yang lebih agresif dan mengirimkan paket penemuan dengan frekuensi yang lebih tinggi. Pada mode *high* dan *aggressive*, XArp menampilkan atau mendeteksi lebih banyak serangan, karena pada mode ini XArp memberikan banyak peringatan serangan palsu disebabkan tingginya frekuensi paket serangan didalam lalu lintas jaringan. Pada hasil scanning yang dilakukan XArp dengan 25 *mappings* ditemukan 17 *alert* serangan ARP. Hasil scanning XArp *tools* terlihat pada Gambar 10.

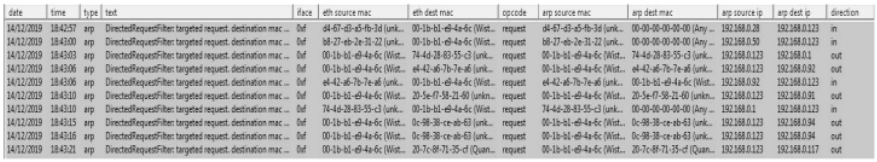


	IP	MAC	Host	Vendor	Interface	Online	Cache	First seen	Last seen
✗	192.168.0.1	74-4d-28-83-55-c3	192.168.0.1	unknown	0xf - Microsoft	unkno...	yes	14/12/2019 18:42:21	14/12/2019 18:46:43
✗	192.168.0.2	b4-fb-e4-40-2d-22	192.168.0.2	unknown	0xf - Microsoft	unkno...	yes	14/12/2019 18:42:21	14/12/2019 18:47:16
✗	192.168.0.3	78-8a-20-d3-bf-7b	192.168.0.3	unknown	0xf - Microsoft	unkno...	yes	14/12/2019 18:42:21	14/12/2019 18:47:06
✗	192.168.0.24	9c-99-a0-01-ed-a9	192.168.0.24	unknown	0xf - Microsoft	unkno...	yes	14/12/2019 18:42:21	14/12/2019 18:42:47
✗	192.168.0.27	48-88-ca-b3-2e-f7	192.168.0.27	unknown	0xf - Microsoft	unkno...	yes	14/12/2019 18:42:21	14/12/2019 18:42:42
✗	192.168.0.28	d4-67-d3-a5-fb-3d	192.168.0.28	unknown	0xf - Microsoft	unkno...	yes	14/12/2019 18:42:21	14/12/2019 18:42:57
✓	192.168.0.30	70-ec-e4-0d-01-b5	192.168.0.30	unknown	0xf - Microsoft	unkno...	yes	14/12/2019 18:42:21	14/12/2019 18:42:21
✗	192.168.0.50	b8-27-eb-2e-31-22	192.168.0.50	unknown	0xf - Microsoft	unkno...	yes	14/12/2019 18:42:21	14/12/2019 18:43:00
✗	192.168.0.91	20-5e-f7-58-21-60	192.168.0.91	unknown	0xf - Microsoft	unkno...	yes	14/12/2019 18:42:22	14/12/2019 18:43:10
✗	192.168.0.92	e4-42-a6-7b-7e-a6	DESKTOP-0M5...	unknown	0xf - Microsoft	unkno...	yes	14/12/2019 18:42:22	14/12/2019 18:43:07
✗	192.168.0.94	0c-98-38-ce-ab-63	192.168.0.94	unknown	0xf - Microsoft	unkno...	yes	14/12/2019 18:42:22	14/12/2019 18:43:16
✓	192.168.0.109	dc-f5-05-76-f1-31	192.168.0.109	unknown	0xf - Microsoft	unkno...	yes	14/12/2019 18:42:22	14/12/2019 18:43:26
✗	192.168.0.117	20-7c-8f-71-35-cf	DESKTOP-UJ8S...	Quanta Micros...	0xf - Microsoft	unkno...	yes	14/12/2019 18:42:22	14/12/2019 18:43:21

XArp 2.2.2 - 25 mappings - 3 interfaces - 17 alerts

Gambar 10. Tampilan hasil scanning XArp *tools*

XArp menampilkan data-data yang diperlukan investigator untuk melakukan investigasi, banyak data yang disajikan pada aplikasi XArp, antara lain tanggal terjadi serangan, waktu terjadi serangan, MAC *Address* penyerang, IP *address* penyerang, MAC *Address victim* dan IP *Address victim*. Hasil deteksi dapat dilihat pada Gambar 11.



date	time	type	text	iface	eth source mac	eth dest mac	opcode	arp source mac	arp dest mac	arp source ip	arp dest ip	direction
14/12/2019	18:42:57	arp	DirectedRequestFilter: targeted request. destination mac ...	0xf	d4-67-d3-a5-fb-3d (unk...	00-1b-b1-e9-4a-6c (Wist...	request	d4-67-d3-a5-fb-3d (unk...	00-00-00-00-00-00 (Any ...	192.168.0.28	192.168.0.123	in
14/12/2019	18:43:00	arp	DirectedRequestFilter: targeted request. destination mac ...	0xf	b8-27-eb-2e-31-22 (unk...	00-1b-b1-e9-4a-6c (Wist...	request	b8-27-eb-2e-31-22 (unk...	00-00-00-00-00-00 (Any ...	192.168.0.50	192.168.0.123	in
14/12/2019	18:43:03	arp	DirectedRequestFilter: targeted request. destination mac ...	0xf	00-1b-b1-e9-4a-6c (Wist...	74-4d-28-83-55-c3 (unk...	request	00-1b-b1-e9-4a-6c (Wist...	74-4d-28-83-55-c3 (unk...	192.168.0.123	192.168.0.1	out
14/12/2019	18:43:06	arp	DirectedRequestFilter: targeted request. destination mac ...	0xf	00-1b-b1-e9-4a-6c (Wist...	e4-42-a6-7b-7e-a6 (unk...	request	00-1b-b1-e9-4a-6c (Wist...	e4-42-a6-7b-7e-a6 (unk...	192.168.0.123	192.168.0.92	out
14/12/2019	18:43:06	arp	DirectedRequestFilter: targeted request. destination mac ...	0xf	e4-42-a6-7b-7e-a6 (unk...	00-1b-b1-e9-4a-6c (Wist...	request	e4-42-a6-7b-7e-a6 (unk...	00-1b-b1-e9-4a-6c (Wist...	192.168.0.92	192.168.0.123	in
14/12/2019	18:43:10	arp	DirectedRequestFilter: targeted request. destination mac ...	0xf	00-1b-b1-e9-4a-6c (Wist...	20-5e-f7-58-21-60 (unkn...	request	00-1b-b1-e9-4a-6c (Wist...	20-5e-f7-58-21-60 (unkn...	192.168.0.123	192.168.0.91	out
14/12/2019	18:43:10	arp	DirectedRequestFilter: targeted request. destination mac ...	0xf	74-4d-28-83-55-c3 (unk...	00-1b-b1-e9-4a-6c (Wist...	request	74-4d-28-83-55-c3 (unk...	00-00-00-00-00-00 (Any ...	192.168.0.1	192.168.0.123	in
14/12/2019	18:43:15	arp	DirectedRequestFilter: targeted request. destination mac ...	0xf	00-1b-b1-e9-4a-6c (Wist...	0c-98-38-ce-ab-63 (unk...	request	00-1b-b1-e9-4a-6c (Wist...	0c-98-38-ce-ab-63 (unk...	192.168.0.123	192.168.0.94	out
14/12/2019	18:43:16	arp	DirectedRequestFilter: targeted request. destination mac ...	0xf	00-1b-b1-e9-4a-6c (Wist...	0c-98-38-ce-ab-63 (unk...	request	00-1b-b1-e9-4a-6c (Wist...	0c-98-38-ce-ab-63 (unk...	192.168.0.123	192.168.0.94	out
14/12/2019	18:43:21	arp	DirectedRequestFilter: targeted request. destination mac ...	0xf	00-1b-b1-e9-4a-6c (Wist...	20-7c-8f-71-35-cf (Quan...	request	00-1b-b1-e9-4a-6c (Wist...	20-7c-8f-71-35-cf (Quan...	192.168.0.123	192.168.0.117	out

Gambar 11. Tampilan data-data hasil *scanning* xARP *tools*

2.4. Analisa

Berdasarkan investigasi forensik yang dilakukan oleh investigator dalam mendeteksi serangan ARP *Spoofing* dengan metode *Live Forensics*, dapat ditemukan beberapa informasi terkait dengan proses identifikasi penyerang, yaitu berupa tanggal terjadi serangan, waktu terjadi serangan, MAC *Address* penyerang, IP *Address* penyerang, MAC *Address victim* dan IP *Address Victim*. Pada tahapan ini semua data yang didapatkan dianalisis untuk mendapatkan informasi terkait serangan sehingga dapat diambil suatu keputusan.

2.5. Laporan

Pada tahap ini diperoleh laporan dari hasil investigasi dan analisis dari simulasi kasus yang telah dilakukan. Beberapa informasi data yang disajikan, tanggal terjadi serangan, waktu terjadi serangan, MAC *Address* penyerang, IP *Address* penyerang, MAC *Address Victim* dan IP *Address Victim*.

3. HASIL DAN PEMBAHASAN

Objek yang diteliti pada penelitian ini adalah serangan ARP *Spoofing* pada jaringan dengan menggun metode *Live Forensics*. Hasil yang disajikan berupa data-data yang diperoleh dari XArp yang dianalisis menjadi informasi yang valid dan tepat. Berdasarkan tahapan skenario dan simulasi dapat dilihat waktu yang dibutuhkan dalam mendeteksi serangan seperti pada Tabel 2.

Tabel 2. Hasil pengujian lama waktu deteksi serangan ARP *Spoofing*

Skenario dan Simulasi	Lama Waktu Deteksi (detik)
PC attacker melakukan satu kali serangan ARP *Spoofing*	0,21
PC attacker melakukan dua kali serangan ARP *Spoofing* dalam waktu yang berbeda	0,30
Dua PC attacker melakukan serangan ARP *Spoofing* dalam waktu yang sama	0,48

Pada tahap skenario dan simulasi dengan menggun *high mode* dan *aggressive mode*, kedepannya dilakukan penelitian untuk memisahkan antara serangan palsu dan serangan ARP asli, sehingga dapat dihitung akurasi dari hasil deteksi serangan ARP *Spoofing*.

4. KESIMPULAN

Berdasarkan hasil penelitian dengan menggun metode *Live Forensics*, investigator dapat dengan cepat mendeteksi suatu serangan dan mengidentifikasi penyerang. Data-data yang diperlukan untuk proses investigasi antar lain, tanggal terjadi serangan, waktu terjadi serangan, MAC *Address* penyerang, IP *Address* penyerang, MAC *Address Victim* dan IP *Address Victim* dapat tersaji dengan cepat dan tepat, sehingga dapat membantu investigator dalam pengambilan keputusan terhadap serangan yang terjadi. Penelitian juga diharapkan dapat memberikan rekomendasi *tools* yang digunakan terutama pada *software* dalam mendeteksi dan mengidentifikasi serangan dan penyerang. Penelitian kedepan juga meneliti cara menangani dan pencegahan dari serangan ARP *Spoofing*.

DAFTAR PUSTAKA

[1] V. Ginting, M. Data, and D. Kartikasari, "Deteksi Serangan ARP *Spoofing* berdasarkan Analisis Lalu Lintas Paket Protokol ARP", vol. 3, no. 5, pp. 5049-5057, June 2019

[2] A. Fadlil, I. Riadi, and S. Aji, "Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan," *Jurnal Ilmu Teknik Elektro Komputer dan Informatika*, vol. 3, no. 1, pp. 11, June 2017

[3] M. S. Ahmad, I. Riadi, and Y. Prayudi, "Investigasi Live Forensik dari Sisi Pengguna untuk Menganalisa Serangan *Man In The Middle Attack* Berbasis Evil Twin," *Ilkom Jurnal Ilmiah*, vol. 9, no. 1, pp. 1-8, 2017. DOI: 10.33096/ilkom.v9i1.103.1-8

[4] D. Mualfah and I. Riadi, "Network Forensics for Detecting Flooding Attack on Web Server," *International Journal of Computer Science and Information. Security (IJCSIS)*, vol. 15, no. 2, pp. 326-331, 2017.

[5] M. I. Mazdadi, I. Riadi, and A. Luthfi, "*Live Forensic*s on RouterOS using API Services to Investigate Network Attacks," *International Journal of Computer Science and Information. Security (IJCSIS).*, vol. 15, no. 2, pp. 406-410, 2017.

[6] R. A. Putra, A. Fadlil, and I. Riadi, "Forensik Mobile pada Smartwatch berbasis Android," *Jurti*, vol. 1, no. 1, p. 41-47, 2017.

[7] A. P. Sujana, "Perangkat Pendukung Forensik Lalu Lintas Jaringan," *Jurnal Teknik Komputer Unikom – Komputika*¸ vol. 3, no. 1, p. 31-37, 2014.

[8] K. Zonggonau and H. Sajati, "Membangun Sistem Keamanan ARP *Spoofing* Memanfaatkan ARPwatch Dan Addons Firefox," *Compiler*, vol. 4, no. 1, pp. 49-58, 2015. DOI: 10.28989/ compiler.v4i1.87

[9] "ARP *Spoofing*." [Online]. Available: https://en.wikipedia.org/wiki/ARP_*Spoofing*.

[10] "ARP *Spoofing* – flaws in network security," 2017. .

[11] A. Kurniawan, "Desain dan Implementasi Aplikasi untuk Visualisasi Informasi pada File Offline Log Web Server," *Jurnal Sistem Informasi,* vol. 4, no. 2, p. 122-128, 2008. DOI: 10.21609/ jsi.v4i2.252

[12] A. R. Supriyono, B. Sugiantoro, and Y. Prayudi, "Live Forensics Acquisition File Sharing Samba pada Mikrotik Router OS,", *Cyber Security dan Forensik Digital*, vol. 1, no. 1, pp. 7–13, 2018.

[13] R. Umar, A. Yudhana, and M. N. Faiz, "Analisis Kinerja Metode *Live Forensic*s Untuk Investigasi Random Access Memory pada Sistem Proprietary," *Prosiding Konferensi Nasional Ke- 4 APPPTM,* Indonesia, 2016, pp. 207–211.

[14] M. N. Faiz, R. Umar, and A. Yudhana, "Implementasi *Live Forensic*s untuk Perbandingan Browser pada Keamanan Email," *JISKA (Jurnal Informatika Sunan Kalijaga)*, vol. 1, no. 3, p. 108-114, 2017. DOI: 10.14421/jiska.2017.13-02

[15] I. Nasrun, "Mengenal IP Versi 6," *IlmuKomputer.Com*, 2005.

[16] D. Susianto and I. Yulianti, "Mengamankan Wireless Dengan Menggun Two Factor, Password dan MAC *Address* Filtering," *EXPERT: Jurnal Sistem Informasi,* vol. 5, no. 2, pp. 31-36, 2015.

37. HASIL CEK_60960140

ORIGINALITY REPORT

12%	12%	0%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	repository.ittelkom-pwt.ac.id Internet Source	4%
2	www.coursehero.com Internet Source	4%
3	dspace.uii.ac.id Internet Source	4%

Exclude quotes	On	Exclude matches	< 4%
Exclude bibliography	On		